HUNTON & WILLIAMS

Overview of U.S. Security Breaches

Protecting Privacy Online: A California Identity Theft Summit
California Department of Consumer Affairs

Lisa J. Sotto
Partner
Hunton & Williams LLP
(212) 309-1223
lsotto@hunton.com

April 11, 2007

Information Security Breaches

- In the U.S., 2005 was the year of the security breach
- Since 2005, nearly 600 information security breaches
  - Choice Point
  - Bank of America
  - Lexis Nexis
  - DSW
  - Card Systems
  - Boston Globe
  - Veterans Administration
  - TJX
- Over 104 million potentially affected
- Over 30 state security breach notification laws
  - California SB 1386 started the trend
- Numerous federal bills

HUNTON& WILLIAMS

State Security Breach Notification Laws

- Generally, the duty to notify arises when unencrypted computerized “personal information” was acquired or accessed by an unauthorized person
- “Personal information” is an individual’s name, combined with:
  - SSN
  - driver’s license or state ID card number
  - account, credit or debit card number, along with password or access code
- But state laws differ:
  - Computerized v. paper data
  - Definition of PI
  - Notification to state agencies
  - Notification to CRAs
  - Timing of individual notification
  - Harm threshold

Recent FTC Enforcement Actions

- FTC enforcement authority: Section 5 of the FTC Act
- Most FTC privacy enforcement actions result from security breaches
  - Card Systems
  - ChoicePoint
  - DSW
  - BJ’s Wholesale Club
  - Petco
  - Tower Records
  - Barnes & Noble.com
  - Guess.com, Inc.
- New Division of Privacy and Identity Protection
- Enforcement trends

What if a Breach Occurs?

- Key question: Does the event trigger notification to individuals?
  - Is it reasonably likely that sensitive PI was “acquired” or “accessed” by an “unauthorized” person?
  - Is an expert evaluation needed to answer this question?

Who are the Stakeholders?

- Recognize the potential stakeholders
  - Board of Directors/senior management
  - Law enforcement
  - Regulators
  - Financial markets
  - Affected individuals
  - Employees
  - Shareholders
  - Auditors
  - Public

Timing of Notification

- If breach notification laws are triggered, when do you notify?
    - In most states, as soon as possible
        - Some states have specified time periods
    - General exceptions
        - Law enforcement delay
        - Investigation and restoration
    - If you rely on exceptions, document the basis for delay

Notification

- Individual notification - Letters must be written with five primary constituencies in mind:
  - Impacted individuals
  - Regulators
  - Plaintiffs’ lawyers
  - Public at large/media
  - Employees
- If you notify under one jurisdiction, notify in all jurisdictions (even foreign)
- Growing “standard” of offerings to affected individuals

The Notice

- Plain language notice – describe:
  - The event
  - Personal information involved
  - Steps taken to protect against further unauthorized acquisition
  - How the company will assist affected individuals
  - Guidance on how individuals can protect themselves from identity theft or account fraud
- Need substantial pre-mailing plan
  - Press statement and related PR
  - Call center set-up, scripts/FAQs and training, then call center monitoring
  - Website materials
  - Credit monitoring arrangement
  - Investor relations

HUNTON& WILLIAMS

Who Else Cares?

- Other interested parties
  - Credit reporting agencies
  - Credit card companies
    - Consider contractual obligations
    - File an incident report
    - Conduct an audit
  - Regulatory agencies
    - FTC and other relevant federal regulators
    - State agencies – NJ, NY, NC, NH, ME, HI, PR
    - Non-U.S. regulators

Lessons Learned

- Prevention is the primary goal, but proactive planning can minimize impact if breach occurs
- Concern and focus on data security must come from the top
- Data breaches often must involve the CEO, CFO, CPO, CIO and GC
- Re-evaluate security systems and policies on an ongoing basis
- Integrate the concern for information security as a core value and train often

Questions?

Lisa J. Sotto
Partner
Head, Privacy and
Information Management
Practice
Hunton & Williams LLP
(212) 309-1223
lsotto@hunton.com